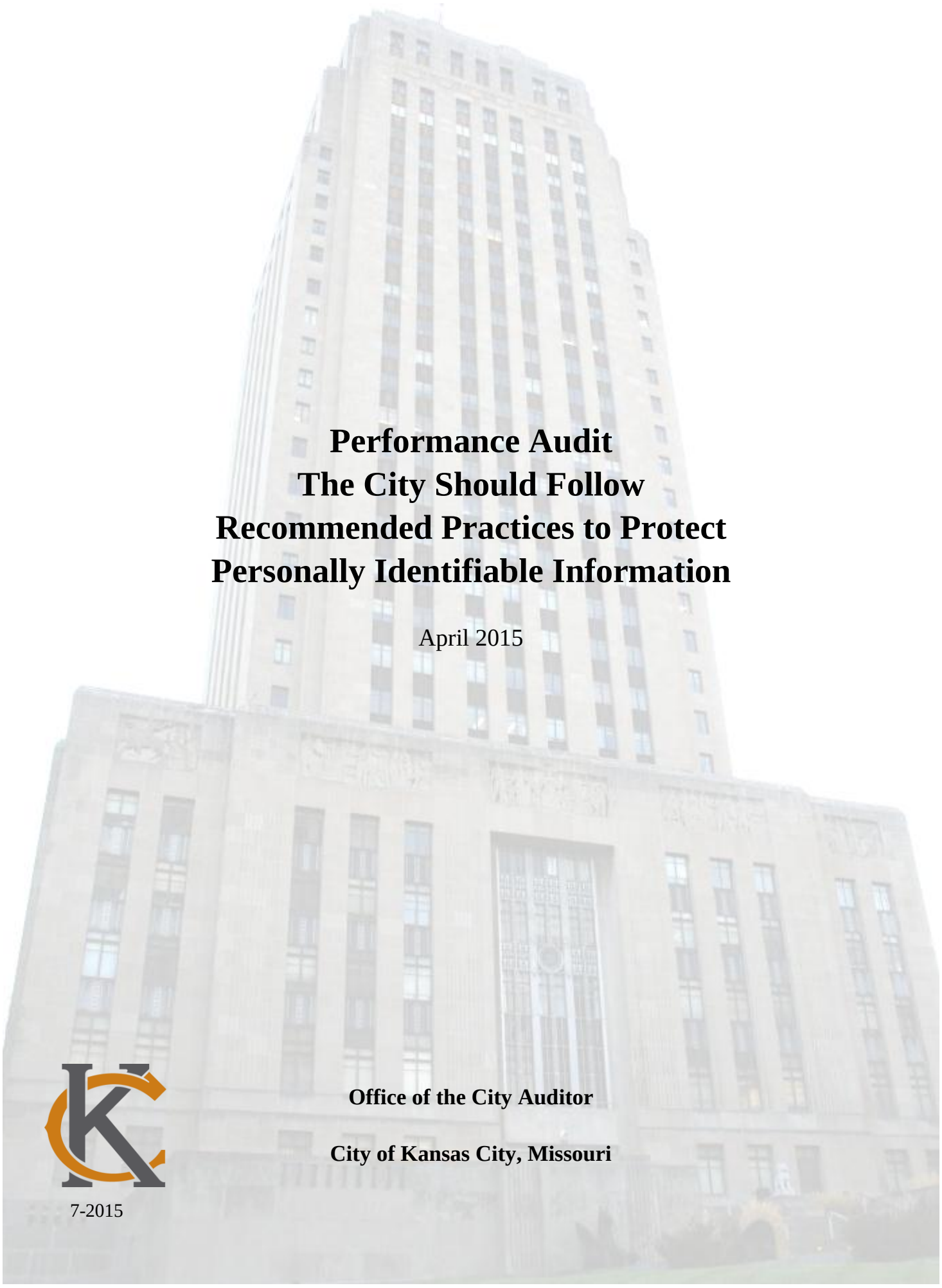

Performance Audit
The City Should Follow Recommended Practices to Protect Personally Identifiable Information

April 2015

Office of the City Auditor

City of Kansas City, Missouri

7-2015

CITY OF FOUNTAINS
HEART OF THE NATION
KANSAS CITY
MISSOURI

Office of the City Auditor

21st Floor, City Hall
414 East 12th Street
Kansas City, Missouri 64106

(816) 513-3300
Fax: (816) 513-3305

April 29, 2015

Honorable Mayor and Members of the City Council:

This audit focuses on whether the city is following recommended practices for protecting personally identifiable information. Personally identifiable information is any information that can be used to identify an individual or can be linked to an individual, such as names, social security numbers, date and place of birth, financial account numbers, medical information, and employment information.

The city collects and maintains a variety of personally identifiable information in both electronic and paper formats. Loss, misuse, or unauthorized disclosure of personally identifiable information could cause individuals to be embarrassed, inconvenienced, and victimized, while the city could lose public confidence, be legally liable, and incur financial consequences.

The city is not following recommended practices related to protecting personally identifiable information. The city has not identified and does not have citywide policies and procedures for protecting the personally identifiable information it collects. However, some departments reported following federal or state regulations. The city's training efforts and safeguards for protecting personally identifiable information are fragmented and need to be strengthened. In addition, the city does not have an incident response plan to handle breaches involving personally identifiable information.

We make recommendations to improve the city's protection of personally identifiable information through identifying what information the city collects, training staff on how to protect it, and applying safeguards.

The draft report was made available to the city manager on April 1, 2015, for review and comment. His response is appended. We would like to thank the city manager and city departments for their assistance and cooperation during this audit. The audit team for this project was Joan Pu, Vivien Zhi, and Nancy Hunt.

Douglas Jones
City Auditor

The City Should Follow Recommended Practices to Protect Personally Identifiable Information

Table of Contents

List of Exhibits

Introduction

Objectives

We conducted this audit of how the city protects personally identifiable information under the authority of Article II, Section 216 of the Charter of Kansas City, Missouri, which establishes the Office of the City Auditor and outlines the city auditor's primary duties.

A performance audit provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision making, and contribute to public accountability.[1]

This report is designed to answer the following question:

- Is the city following recommended practices for protecting personally identifiable information that it collects and maintains?

Scope and Methodology

Our review focuses on whether the city is following recommended practices for protecting personally identifiable information. Our audit methods included:

- Reviewing the U.S. Department of Commerce's National Institute of Standards and Technology's *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* and the U.S. Department of Homeland Security's *Handbook for Safeguarding Sensitive Personally Identifiable Information* to identify criteria and recommended practices related to protecting personally identifiable information.

[1] Comptroller General of the United States, *Government Auditing Standards* (Washington, DC: U.S. Government Printing Office, 2011), p. 17.

- Reviewing Missouri state statutes and the Office of the Missouri Secretary of State's *Missouri Local Government Records Management Guidelines* to identify provisions and guidelines related to protecting personally identifiable information.

- Reviewing the city's Code of Ordinances, Administrative Regulations, Manual of Instructions, and Records Control Guidebook to identify city policies and procedures related to protecting personally identifiable information.

- Conducting an on-line survey of city human resource liaisons, fiscal officers, records coordinators, and management to identify city departments' practices for protecting personally identifiable information.

- Analyzing survey results to understand city practices in protecting personally identifiable information.

- Interviewing the city's chief information officer, the manager of records and information management office, and a member of the Records Control Committee to determine how the city protects personally identifiable information in paper and electronic formats.

- Comparing city practices for protecting personally identifiable information with recommended practices.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. No information was omitted from this report because it was deemed privileged or confidential.

Background

Personally Identifiable Information

Personally identifiable information is any information that can be used to identify an individual or can be linked to an individual. Examples of personally identifiable information include names, addresses, social security numbers, date and place of birth, photos, financial account numbers, medical information, and employment information.

Survey of Personally Identifiable Information Collected and Maintained by City Departments

We conducted an on-line survey about the city's practices in protecting personally identifiable information from loss, misuse, or unauthorized disclosure. We sent 149 survey invitations to human resource liaisons, fiscal officers, records coordinators, and management in each of city's 20 departments in February 2015 and received valid responses from 50 percent of those we surveyed. (See Exhibit 1.)

Exhibit 1. Survey Responses by Position

Position	Number of Responses[2]	Response Rate
Human Resources Liaison	11	55%
Fiscal Officer	12	60%
Records Coordinator	12	63%
Department Management	52	48%

Source: City Auditor's Office survey and analysis.

The survey asked about five types of personally identifiable information that could be collected and stored by city departments, whether in electronic or paper format:

- Social security number,
- Date of birth,
- Bank account information,
- Credit card number, and
- Medical information.

[2] Some city departments have one person filling multiple roles (e.g. human resources liaison and fiscal officer). Some survey responses were counted more than once in this table when the individual filled more than one role within a department.

Findings and Recommendations

City Needs to Take Steps to Protect Personally Identifiable Information

Although the city collects a variety of personally identifiable information, it has not identified all that it collects, uses, and stores. In addition, the city does not have citywide policies and procedures for protecting personally identifiable information. The city's training effort for handling personally identifiable information is fragmented. Safeguards for protecting personally identifiable information need to be increased. Furthermore, the city needs to implement an incident response plan to ensure it responds appropriately to breaches involving personally identifiable information.

City Should Identify All Personally Identifiable Information It Collects, Uses, and Stores

The city has not identified all personally identifiable information it collects, uses, and stores. To determine what types of information the city collects, we surveyed staff from each department and asked them whether they collected some common personally identifiable information, including dates of birth, social security numbers, medical information, bank account information, and credit card numbers. All city departments that responded to our survey collect and store at least two types of personally identifiable information. Almost 75 percent of the responding departments reported collecting and storing four or more types of the personally identifiable information we included in our survey. (See Exhibit 2.) Most departments reported that the primary uses of the information were for employment and payment processing purposes.

Exhibit 2. Personally Identifiable Information Collected and Stored by Departments

Department	Date of Birth	Social Security Number	Medical Information	Bank Account Information	Credit Card Number
Aviation	●	●	●	●	
City Auditor's Office	●	●	●	●	
City Clerk	●	●			
City Manager's Office	●	●			
City Planning & Development	●	●	●	●	●
Convention & Entertainment Facilities	●	●	●	●	●
Finance	●	●	●	●	●
Fire	●	●	●	●	●
General Services	●	●	●	●	●
Health	●	●	●	●	
Human Relations	●	●	●	●	●
Human Resources	●	●	●		
Law	●	●	●		
Mayor's Office	●		●		
Municipal Court	●	●	●	●	●
Neighborhood & Housing Services	●	●		●	●
Parks & Recreation	●	●	●	●	●
Public Works	●	●	●	●	
Water Services	●	●	●	●	
Number of Departments	19	18	16	14	9

Source: City Auditor's Office survey.

The National Institute of Standards and Technology (NIST) recommends that organizations identify all personally identifiable information maintained within its environment or under its control.[3] To properly protect personally identifiable information, an organization needs a clear understanding of the amount, types, locations, and accessibility of all the personally identifiable information it collects, stores, and uses. Although our survey only asked about five types of personally identifiable information, departments likely collect and store additional information that could also be classified as personally identifiable information. (See Appendix A for examples of personally identifiable information.)

NIST also recommends that the confidentiality of personally identifiable information be protected based on its confidentiality impact level – the potential harm or adverse effects that would be experienced by an individual or by the organization from which the information was

[3] National Institute of Standards and Technology (NIST), U.S. Department of Commerce, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Special Publication 800-122, April 2010, p. 2-1.

inappropriately accessed, used, or disclosed.[4] The factors that can be used to determine the impact levels include the nature of the information or how easily the information can be used to identify specific individuals; the quantity of the information or the number of individuals that can be identifiable in the information; the purposes for which the information is collected, stored, and used; laws, regulations, or other mandates governing the obligation to protect the information; and access to and locations of the information or how frequently and widely the information is accessed and where the information is stored.

As the first step in protecting personally identifiable information, the city manager should identify all personally identifiable information the city collects and stores and evaluate the confidentiality impact level of the information so that appropriate safeguards can be instituted.

Managing the personally identifiable information the city collects can limit exposure if a breach occurs. Although the personally identifiable information that we asked about in our survey appears relevant to city functions, regularly reviewing the personally identifiable information the city collects can determine whether the information is still needed for city business purposes.

NIST recommends that organizations minimize the collection and retention of personally identifiable information to what is necessary to accomplish their business purpose and mission.[5] NIST advises that organizations regularly review the personally identifiable information they collected and maintained to make sure the information is still needed to meet their business purposes. Collecting and retaining unnecessary personally identifiable information increases the risk of unauthorized access and disclosure and the costs associated with storing and safeguarding that information.

To reduce the risk of mishandling personally identifiable information and the cost of storing and safeguarding unnecessary information, the city manager should periodically review the personally identifiable information collected and maintained by the city to determine whether the information is necessary to meet the city's business purposes and eliminate the collection of unnecessary personally identifiable information.

[4] NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, p. 3-1.
[5] NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, p. 4-3.

City Should Apply Safeguards for Personally Identifiable Information

The city does not have citywide policies and procedures for protecting personally identifiable information. Roles and responsibilities for protecting the information are not clear. The city's training effort for handling personally identifiable information is fragmented. Safeguards over personally identifiable information need to be increased.

A comprehensive citywide policy is needed. The city does not have citywide policies and procedures for protecting personally identifiable information. NIST recommends organizations develop comprehensive policies and procedures for handling personally identifiable information.[6] Although current city policies and procedures cover some aspects of protecting personally identifiable information, they do not cover enough.

Personally identifiable information policy needs to cover all aspects of protecting information. The city's records management program has policies and procedures covering record storage, retention, and disposal, including the handling of confidential information.[7] Administrative Regulation 1-16 includes information related to protecting city data, such as encrypting confidential data, role security, locking computer screens, physical access control to the data center, and rules for using portable devices and personally owned device.

We found that no departments have written policies and procedures covering the collection, access, storage, and disposal of personally identifiable information. Many departments responding to our survey referred to the city's Administrative Regulation and Manual of Instructions for records control as their department's policy and procedures for protecting personally identifiable information. Some departments reported following federal or state regulations.[8] One department requires employees to sign a confidentiality disclosure and inspection statement, which states the employee's responsibilities for maintaining confidential and personal employee and applicant information. These regulations and policies and procedures do not cover every stage of protecting personally identifiable information. Some of them cover the storage, retention, and disposal of confidential information, some cover the access and disclosure of confidential

[6] NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, p. 4-1.
[7] *Administrative Regulations 3-22*, "Records and Information Management," January 2014. *Manual of Instruction 3-28*, "Records Management Instructions," January 2005.
[8] The federal regulations include Health Insurance Portability and Accountability Act (HIPAA) and U.S. Department of Housing and Urban Development (HUD), U.S. Equal Employment Opportunity Commission (EEOC), and Internal Revenue Service (IRS) regulations. In addition, Missouri has records retention regulations.

information, and some only cover certain types of personally identifiable information. A comprehensive citywide policy should include every aspect of protecting personally identifiable information, including collection, access, storage, and disposal.

Roles and responsibilities need to be defined. NIST recommends organizations clearly define roles and responsibilities for protecting personally identifiable information.[9] Our survey asked whether someone was responsible for the oversight and security of personally identifiable information collected or stored by their department. About one third of the respondents reported no one was responsible or they did not know whether someone in their departments was responsible. Over two thirds of the respondents reported someone is responsible, but the named individuals varied by positions within their departments and sometimes included divisions outside of their departments. Comprehensive citywide policies and procedures for handling personally identifiable information should define roles and responsibilities for protecting the information.

Training and awareness efforts will help protect personally identifiable information. NIST recommends organizations reduce the possibility that personally identifiable information will be accessed, used, or disclosed inappropriately by requiring that all individuals receive appropriate training before being granted access to systems containing the information.[10] Over half of the survey respondents reported their departments do not provide training to employees before they are granted access to the information or they do not know whether their departments have such training. Awareness and training can change city staff behavior, enforce desired practices, and build knowledge and skill to protect information collected and maintained by the city.

The city should ensure access to personally identifiable information is restricted. NIST recommends organizations protect personally identifiable information through access control.[11] About one out of four survey respondents reported there are no restrictions or they do not know whether access to the personally identifiable information is restricted in their departments. The restrictions reported by the respondents are often related to physical access, such as information being kept in locked cabinets or areas or kept by designated staff. Other restrictions include log-in access (ID and password) for electronic files, access restricted to division or department staff, following federal or state law and

[9] NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, p. 4-3.
[10] NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, p. 4-2.
[11] NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, p. 4-7.

regulations, passing special background checks, and staff signing confidentiality disclosure statements.

The city's chief information officer told us that strict physical security is applied to the city's data center. All city employees have access to the city's network and PeopleSoft self-service, but any other access to the city's network and servers requires requests from the employee's department and approval by the Finance and Human Resources departments. Both departments periodically request that departments review their employees' access to PeopleSoft systems. Information Technology Division (ITD) also destroys hard drives of retired computers.

The city uses some methods to protect confidential information, but more safeguards are needed. NIST recommended using a combination of different safeguards to reduce the possibility that personally identifiable information will be accessed, used, or disclosed inappropriately.[12] Safeguards could include de-identifying, anonymizing, and encrypting personally identifiable information. De-identifying or anonymizing records removes enough personally identifiable information so that the remaining information does not identify an individual when full records are not necessary. The city has implemented some de-identifying mechanisms on personally identifiable information. For example, when processing credit card payments, the city's system only keeps the last four digits of the credit card numbers.

ITD encrypts the Revenue Division's laptops to protect IRS data. The city, however, does not encrypt personally identifiable information saved on other laptops. Employees can contact ITD to have an encryption program installed on laptops, but this is not required.

The city's chief information officer told us that the city's email system blocked email messages containing social security numbers. We tested system security by sending out numbers in the format of a social security number to email addresses outside and inside of city hall. The emails reached the recipients. We notified ITD about our testing and ITD subsequently fixed the problem.

To ensure personally identifiable information the city collects and stores is adequately safeguarded, the city manager should develop citywide policies and procedures for protecting the confidentiality of the information, including training and a combination of safeguarding controls.

[12] NIST *Guide to Protecting the Confidentiality of Personally identifiable Information (PII)*, pp. 4-1, 4-6.

Safeguarding Sensitive Personally Identifiable Information (PII)

The U.S. Department of Homeland Security (DHS) provides its employees the following guidelines for protecting personally identifiable information.

When employees handle, process, transmit, transport and/or store sensitive PII, employees should limit the potential for unauthorized disclosure. For example, employees should protect against "shoulder surfing" or eavesdropping by being aware of one's surroundings when processing or discussing PII.

PII in Electronic Form:
Sensitive PII should only be accessed via DHS-approved, encrypted portable electronic devices such as laptops, USB flash drives, and external hard drives. Personally-owned USB flash drives may not be used. Personally-owned computers should not be used to access, save, store, or host sensitive PII unless logging in through the organization's virtual desktop.

Transporting PII:
Employees should obtain supervisor authorization before removing documents containing sensitive PII from the workplace. Employees should physically secure the information when in transit, such as encrypting the electronic data before mail or courier. Employees should not pack laptops or electronic storage devices in checked baggage or leave in a car for an extended period of time. Employees should never leave paper files or electronic devices in plain sight in an unattended vehicle.

Hard Copy PII in Workplace:
Employees should never leave sensitive PII in hard copy unattended and unsecured. Employees should physically secure (e.g. in a locked drawer, cabinet, desk, or safe) sensitive PII when not in use or not otherwise under the control of a person with a need to know. Employees should try not to send sensitive PII using a fax machine.

Emailing PII Within DHS
Employees should password-protect or encrypt sensitive PII when emailing within the DHS. Employees can also redact the sensitive PII before emailing.

Emailing PII Outside of DHS:
Employees should email the sensitive PII within an encrypted attachment with the password provided separately (e.g. by phone, another email, or in person).

Storing PII on a Shared Drive:
Employees should store sensitive PII on shared network drives only if access is restricted to those with a need to know by permissions settings or passwords.

Source: U.S. Department of Homeland Security, *Handbook for Safeguarding Sensitive Personally Identifiable Information*, March 2012.

City Should Develop an Incident Response Plan

The city does not have an incident response plan to handle breaches involving personally identifiable information. Almost 75 percent of the survey respondents said their departments do not have a written plan to respond to incidents of misuse, unauthorized disclosure or access, or other breaches of personally identifiable information or they do not know whether their department has such a plan.

NIST recommends that organizations develop an incident response plan to handle breaches involving personally identifiable information.[13] An effective incident response plan and response capabilities should address preparation; detection and analysis; containment, eradication and recovery; and post-incident activities. The plan should cover personally identifiable information in both electronic and paper formats and include elements such as determining when and how individuals should be notified, how a breach should be reported, and whether to provide remedial services, such as credit monitoring to affected individuals.

In order to respond to incidents involving the loss or compromise of personally identifiable information quickly, consistently and effectively, the city manager should develop a response plan for incidents of misuse, unauthorized disclosure or access, or other breaches of personally identifiable information.

[13] NIST *Guide to Protecting the Confidentiality of Personally identifiable Information (PII),* p. 5-1.

Recommendations

1. The city manager should identify all personally identifiable information the city collects and stores and evaluate the confidentiality impact level of the information.

2. The city manager should periodically review and eliminate the collection of unnecessary personally identifiable information.

3. The city manager should develop citywide policies and procedures, including training and other safeguarding controls, for protecting the confidentiality of the personally identifiable information.

4. The city manager should develop a response plan for incidents of misuse, unauthorized disclosure or access, or other breaches of personally identifiable information.

Appendix A

Examples of Personally Identifiable Information

Examples of Personally Identifiable Information

The following list contains examples of information that may be considered personally identifiable information either singly or collectively:

- Name
  - Full name
  - Maiden name
  - Mother's maiden name
  - Alias
- Personal identification number
  - Social security number
  - Passport number
  - Driver's license number
  - Taxpayer identification number
  - Financial account number
  - Credit card number
  - Patient ID number
- Address information
  - Street address
  - Email address
- Asset information
  - Internet Protocol (IP) address
  - Media Access Control (MAC) address
- Telephone numbers
  - Mobile phone numbers
  - Business phone numbers
  - Personal phone numbers
- Personal characteristics
  - Photographic image (especially face or other identifying characteristic)
  - Fingerprints
  - X-rays
  - Handwriting
  - Other biometric data (e.g. retina scan, voice signature, facial geometry)
- Information identifying personally owned property
  - Vehicle registration
  - Title number
- Information about an individual that is linked or linkable to one of the above
  - Date of birth
  - Place of birth
  - Race
  - Religion
  - Weight
  - Activities
  - Geographical indicators
  - Employment information
  - Medical information
  - Education information
  - Financial information
  - Criminal history

Source: National Institute of Standards and Technology, U.S. Department of Commerce, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.

Appendix B

City Manager's Response

CITY OF FOUNTAINS
HEART OF THE NATION

KANSAS CITY
MISSOURI

Inter-Departmental Communication

Office of the City Manager

RECEIVED
APR 28 2015
CITY AUDITOR'S OFFICE

Date: April 27, 2015

To: Douglas Jones, City Auditor

From: Troy M. Schulte, City Manager

Subject: Response to Performance Audit: *The City Should Follow Recommended Practices to Protect Personally Identifiable Information*

1. ***The city manager should identify all personally identifiable information the city collects and stores and evaluate the confidentiality impact level of the information.***

Agree. Work on this effort began with this audit and will be incorporated into a new Administrative Regulation.

2. ***The city manager should periodically review and eliminate the collection of unnecessary personally identifiable information.***

Agree. This review has begun and the findings will be incorporated into a new Administrative Regulation.

3. ***The city manager should develop citywide policies and procedures, including training and other safeguarding controls, for protecting the confidentiality of the personally identifiable information.***

Agree. The department directors that collect the most sensitive data have been tasked to develop a new administrative regulation that will outline the policies and procedures that will govern the collection of personally identifiable information.

4. ***The city manager should develop a response plan for incidents of misuse, unauthorized disclosure or access, or other breaches of personally identifiable information.***

Agree. This response plan will be incorporated into a new administrative regulation.